Department of Veterans Affairs
Washington, DC 20420

VA Handbook 6210
Transmittal Sheet
January 30, 1997

AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY PROCEDURES

1. **REASON FOR ISSUE:** This handbook establishes procedures and practices for AIS security programs at all organizational levels of the Department of Veterans Affairs. It implements the policies contained in VA Directive 6210, Automated Information Systems Security.

2. **SUMMARY OF CONTENT/MAJOR CHANGES**

a. The Automated Information Systems (AIS) Security Procedures Handbook provides the general procedures and guidelines to implement the policies contained in VA Directive 6210, Automated Information Systems Security.

b. Provides guidance on key AIS security topics, such as business resumption and contingency planning, computer security training, security incident reporting, viruses, copyright, information stored on automatic data processing equipment during disposal, and local area network security.

c. Provides a comprehensive reference document addressing the minimum security standards required to guide the conduct of VA Administrations' and Staff Offices' activities directed toward their AIS program.

d. Consistent with the requirements of OMB Circular No. A-130, Appendix III, dated February 8, 1996, the Amendment:; to the Computer Security Act of 1987, (PL 100-235) and OMB Bulletin No. 90-08, dated July 9, 1990.

3. **RESPONSIBLE OFFICE:** The Office of the Associate Deputy Assistant Secretary for Policy and Program Assistance (045A), Office of the Deputy Assistant Secretary for Information Resources Management.

4. **RELATED DIRECTIVE:** VA Directive 6210, Automated Information Systems Security.

5. **RESCISSION:** MP-6, Part I, Chapter 2, Change 18, dated February 24, 1992.

CERTIFIED BY:

Nada D. Harris
Deputy Assistant Secretary for
Information Resources Management

BY DIRECTION OF THE SECRETARY
OF VETERANS AFFAIRS:

D. Mark Catlett
Assistant Secretary for Management

Distribution: RPC: **6500**
FD

CONTENTS

CHAPTER 1. BUSINESS RESUMPTION AND CONTINGENCY PLANNING PROCEDURES

PARAGRAPH PAGE

CHAPTER 2. COMPUTER SECURITY TRAINING PROCEDURES

PARAGRAPH

CHAPTER 3. SECURITY INCIDENT REPORTING PROCEDURES

PARAGRAPH

CHAPTER 4. VIRUS CONTROL PROCEDURES

PARAGRAPH

CHAPTER 5. COPYRIGHT SECURITY PROCEDURES

PARAGRAPH PAGE

CHAPTER 6. PROCEDURES FOR SAFEGUARDING SENSITIVE INFORMATION STORED ON AUTOMATIC DATA PROCESSING EQUIPMENT DURING DISPOSAL

PARAGRAPH

CHAPTER 7. LOCAL ARE.9 NETWORK SECURITY PROCEDURES

PARAGRAPH

APPENDICES

CHAPTER 1. BUSINESS RESUMPTION AND CONTINGENCY PLANNING PROCEDURES

1. **PURPOSE and SCOPE.** This chapter establishes mandatory operational requirements for business resumption and contingency planning within the Department of Veterans Affairs. It is designed to provide Department-wide guidance to VA Administrations and Staff Offices in responding to catastrophic events involving VA facilities and information technology service interruptions.

2. BACKGROUND. Traditionally, contingency planning has focused on restoring information technology services for an automation center, wide area network or similar service. While remote sites are still accessed for processing and storing information, most VA facilities including: VACO, regional offices, and medical centers, have their own local area networks which link the various personal computers and share various resources. If a catastrophic event occurs that makes it impossible for VA employees to use that site, the re-establishment of information systems and network functions is only one part of the resumption of services for a facility. The critical functions of that facility must be restored and an interim process must be put into action. "Hot sites" (a reserved space already equipped with processing capability and other services), reciprocal agreements, and other arrangements to provide restored services to their end users should be considered. Critical files that were processed previously on Local Area Network servers need to be restored so they can be used in processing during the contingency period. In summary, both the information technology and the general office environment have to be restored.

3. **RESPONSIBILITIES**

a. The VA Chief Information Officer (CIO) is charged with ensuring that a business resumption plan is developed at all VACO locations. This includes the necessary contingency plans for critical automated information systems. The CIO is also responsible for monitoring, reviewing, and evaluating compliance with this automated information system (AIS) security program directive. These responsibilities are redelegated to the VA Information Resources Security Officer (IRSO) for execution.

b. Administration heads, Assistant Secretaries, Deputy Assistant Secretaries and other key officials are responsible for ensuring that offices and facilities under their control can operate despite disruptions. These offices and facilities must include business resumption and contingency planning as vital considerations in their computer security programs in protecting sensitive information in VA automated information systems.

c. The director of each VA field station is responsible for the development, periodic testing and updating of a business resumption plan for that field station and contingency plans for all general support systems located at that field station.

4. PROCEDURES. The following procedures outline the steps to be followed in the development and implementation of an effective business resumption and contingency plan for VA organizations and facilities. A recommended resource to use in the organizing, developing, testing, and implementing a contingency plan is VHA's "VA Medical Center Contingency Planning Boilerplate." This document provides a blueprint for the creation of contingency plan policies and procedures; it also includes sample forms used to document each step. Additional information concerning this contingency planning outline may be obtained by contacting the Medical Information Security Service at the National Center for Information Security, at VAMC Martinsburg, WV.

a. Identify **Mission Critical Functions.** The first step of business resumption planning is to identify mission critical functions and determine their priorities. In the event of a disaster, certain functions will not be performed. If appropriate priorities have been set and approved by senior management, it will be easier for the organization to recover from the disaster and resume normal operations. Contingency plans shall be consistent with other site and building emergency plans. All plans designed to continue essential VA missions and functions must be coordinated with each other and recognize the dependent nature of this process.

b. **Identify the Resources that Support Critical Functions.** After mission critical functions are identified, the resources to support the critical functions must be identified, determine the time frames in which each resource is used (some are needed daily and others are used only once a month), and to determine the effect on the mission if the resource is not available. One method used to identify mission-critical functions and their impact is called Business Impact Analysis. It includes a review of the site's functions to understand the impact if they are not performed. A review is done of each function regarding its impact on operations, end users, interrelationships with other critical functions, as well as time lines and considering workload peaks and valleys. Also considered are additional expenses caused by overtime, the need for temporary employees and other costs associated with recovery. Finally, the effect of not performing a mission critical function needs to be examined and considered with regard to its impact within the organization, externally, and in the media.

c. **Anticipating Potential Contingencies or Disasters.** All resources associated with critical functions should be examined with likely problem scenarios. Various types and sizes of contingencies should be considered. To better understand resource needs and their support of critical functions, a contingency planning team should be formed. Team members should include representatives from three main areas: functional/business groups, facilities management, and technology management. Legal advisors and other specialty groups can be assigned as needed to the team. This assignment should not preclude members of these groups from serving in other planning roles. Members from these areas may include financial management, personnel, computer security, and physical security. The team should identify likely problems by using analytical tools, such as existing risk assessment methodologies (e.g., qualitative and quantitative, outlined in FIPS Publication 65), and risk assessment software packages. A Department reference on the assessment of risk is found in VHA Manual, M-11, Information Resources Management, Chapter 16.

d. **Selecting Business Resumption and Contingency Planning Strategies.** The primary purpose of this step is to plan how to recover needed resources. Alternative strategies should be evaluated to consider what controls are in place to prevent and minimize contingencies.

(1) A contingency planning strategy normally consists of three parts: emergency response, recovery, and resumption. E:nergency response encompasses the initial actions taken to protect lives and limit damage. Recovery refers to the steps that are taken to continue support for critical functions. Resumption is the return to normal operations. The relationship between recovery and resumption is important. The longer it takes to resume normal operations, the longer the organization will have to operate in the recovery mode.

(2) The selection of a strategy needs to be based on practical considerations as feasibility and cost. Risk assessment can be used to help estimate the cost of options to decide on an optimal strategy. Questions to be asked are: Is it more expensive to purchase and maintain a generator or to move processing to an alternate site, considering the likelihood of loosing electrical power for various lengths of time? Are the consequences of loss of computer-related resources sufficiently high to warrant the cost of various recovery strategies? The risk assessment should focus on areas where it is not clear which strategy is the best. In developing contingency planning strategies, there are many factors to consider in addressing each of the resources that support critical functions. The different categories of resources should each be considered. Some of these factors include: human

resources, processing capability, automated applications and data, computer-based services, physical infrastructure, documents and papers.

(a) **Implementation**

(1) Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources. For example, one common preparation is to establish procedures for backing up files and applications. Another is to establish contracts and agreements, if the contingency strategy calls for them. Existing service contracts may need to be re-negotiated to add contingency services. Another preparation may be to purchase equipment, to support a redundant capability.

(2) Backing up data files and applications is a critical part of virtually every contingency plan. Backups are used to restore files after a personal computer virus corrupts the data or after a hurricane destroys an automation center. System backups must be tested on a regular basis to ensure that data can be read from the disks in the event they are needed in an emergency.

(3) It is important to keep preparations, including documentation, up-to-date. Computer systems change rapidly and backup services and redundant equipment should also be kept current. Contracts and agreements also need to reflect any changes. If additional equipment is needed, it must be maintained and periodically replaced when it is no longer dependable or obsolete to an organization's architecture.

(4) Preparation should also include formally designating people who are responsible for various tasks in the event of a contingency. These people are often referred to as the contingency response team. This team is often composed of people who were also members of the contingency planning team.

(5) There are many important implementation issues for an organization to consider. Two of the most important are 1) how many plans should be developed and 2) who will prepare each plan. The answer will depend on the organization's overall strategy for contingency planning, and should be documented in the organization's policy and procedures document.

(6) For small or less complex systems, the contingency plan may be a part of the computer security plan. For larger complex systems, the computer security plan could contain a brief synopsis of the contingency plan, which should be a separate document. The purpose of the computer security plan is to provide a basic overview of the security and privacy requirements for a computer system and the responsible VA component's plan for meeting those cequirements. It also serves as documentation of the process of planning adequate, cost-effective security protection for a system. The purpose of the contingency plan is to document the specific methodology, structure, discipline, and procedures to be used for emergency response, backup operations, and post-'disaster recovery maintained by the responsible VA office as part of its AIS security program. This planning will help ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

(7) Some organizations have one plan for the entire organization; others have a plan for each distinct computer system,, application, or other resource. Other approaches recommend a plan for each business or mission function, with separate plans, as needed, for critical resources.

(8) The number of actual plans needed depends upon the unique circumstances for each organization. Coordination and cooperation between resource managers and functional managers responsible for the mission or business is critical to the success of any plan.

(b) **Documentation.** The contingency plan needs to be: documented, kept up-to-date as the personnel responsible for implementation of the contingency plan and other factors change. A written plan is essential to have during a contingency situation. It should clearly state in simple language sequence of tasks to be performed in the event of a contingency so that someone with minimal knowledge can immediately begin to execute the plan. It is important to store, in a secure environment, up-to-date copies, including one in electronic format, of the contingency plan in several locations, including any off-site locations, such as alternate processing sites or backup data storage facilities. Each member of the contingency plan response team should have copies of the plan.

(c) Training. All personnel should be trained in their contingency-related duties. New personnel should be trained as they join the organization. Refresher training may be needed and personnel need to practice their skills. Training is particularly important for effective employee response during emergencies. Depending on the nature of the emergency, there may be inadequate time to check a manual to determine correct procedures to protect equipment and other assets. Practice is necessary in order to react correctly, especially when human safety is involved.

e. Testing and Revising

(1) A contingency plan should be tested periodically to identify and correct any problems in implementation. The plan will become dated as time passes and as the resources used to support critical functions change. Responsibility for keeping the contingency plan current should be specifically assigned. The extent and frequency of testing will vary between organizations and among systems, There are several types of testing, including reviews, analyses, and simulations of disasters.

(a) A review can be a simple test to check the accuracy of contingency plan documentation. For instance, a reviewer could check if individuals listed are still in the organization and still have the responsibilities that caused them to be included in the plan. This test can check home and work telephone numbers, organizational codes, and building and room numbers. The review can determine if files can be restored from backup tapes or if employees know emergency procedures.

(b) An analysis may be performed on the entire plan or portions of it, such as emergency response procedures. It is more beneficial if the analysis is performed by a member of the facility staff who did not participate in the development of the contingency plan, but has a sound knowledge of the critical functions and supporting resources. This person may also interview functional managers, resource managers, and their staff to uncover missing or unworkable sections of the plan.

(c) Organizations may also arrange disaster simulations. These tests provide valuable information about flaws in the contingency plan and provide practice for a real emergency. While they can be expensive, these tests can also provide critical information that can be used to ensure the continuity of important functions. In general, the more critical the functions and the resources addressed in the contingency plan, the more cost-beneficial it is to perform a disaster simulation.

(2) The results of a "test" often imply a grade assigned for a specific level of performance, or simply pass or fail. However, in the case of contingency planning, a test should be used to improve the plan. If organizations do not use this approach, flaws in the plan may remain undetected and not corrected.

f. **Interdependencies.** Controls can prevent or reduce the effects of a disaster at the facility. Ideally, controls mutually support and compliment each other. In combination, they eliminate or lessen the damage occurring as a result of the destruction, disclosure, or denial of service to critical resources.

(1) Risk assessment provides a tool (process) for analyzing the security costs and benefits of various contingency planning options. In addition, **a** risk assessment effort can be used to help identify critical resources needed to support

the organization and the likely threat to those resources. It is not necessary, however, to perform a risk assessment prior to contingency planning, since the identification of critical resources can be performed during the contingency planning process itself.

(2) Physical and environmental controls help prevent the destruction of automated information systems, although many of the other controls, such as logical access controls, also prevent damage. The main threats that a contingency plan address are physical such as: fires; loss of power; plumbing breaks; and natural disasters.

(3) Incident handling can be viewed as a subset of contingency planning. It is the emergency response capability for {various technical threats. Incident handling can also help an organization prevent future incidents by recording the incident and educating personnel about the incident,. the circumstances, and the corrective action taken.

(4) Support and operations in most organizations include the periodic backing up of critical files. It also includes the prevention and recovery from more common contingencies, such as a disk failure or corrupted data files.

(5) Policy is needed to create and document the organization's approach to contingency planning. The policy should explicitly assign responsibilities.

g. Cost Considerations. The cost of developing and implementing contingency planning strategies should be taken into account and, when included in the strategy, additional expenses for contracting backup services or duplicate equipment. One contingency cost that is often overlooked is the cost of testing a plan. Testing provides many benefits and should be parformed, although some of the less expensive methods (such as a review) may be sufficient for less critical resources.

5. REFERENCES

a. National Institute of Standard:; and Technology, Gu idelines for ADP Contingency Planning, FIPS Pub 87; 1981.

b. VA Directive 0320, Emergency Preparedness Planning.

CHAPTER 2. COMPUTER SECURITY TRAINING PROCEDURES

1. PURPOSE. Computer security training requirements shall be developed and conducted for all VA employees involved with the management, use or operation of each VA computer system which contains sensitive data. The procedures and responsibilities described in this handbook apply to all VA elements and to non-VA organizations that use VA computer systems, including contractors performing work for VA. Each organization is responsible for conducting annual AIS security training to raise the level of AIS security in VA. This Chapter focuses on the provision for development and implementation of a security awareness and training program for VA.

2. BACKGROUND. The Computer Security, Act of 1987 was signed and became Public Law 100-235 on January 8, 1988. The Act strengthens the role and responsibility of the National Institute of Standards and Technology for the development and promulgation of computer security. The Act places emphasis on three major provisions:

(1) Identifying computer systems containing sensitive information;

(2) Developing security plans for those sensitive systems;

(3) Mandating computer security training for all users of sensitive Federal computer systems.

3. RESPONSIBILITIES

a. The Secretary of Veterans Affairs is responsible for AIS security in VA.

b. The VA CIO is responsible for implementing the Computer Security Act of 1987 and related OPM regulations through the VA's automated information systems security program. The CIO will ensure that computer security training and awareness are basic elements of the VA's AIS security program.

c. The Information Resources Security officer (IRSO) for VA, is responsible for:

(1) Ensuring that appropriate Department policy complies with the computer security training requirements of the Computer Security Act of 1987 and related implementing regulations.

(2) Developing and issuing procedures for VA components' use to organize and conduct computer security and awareness training for all employees.

d. Administration Heads, Assistant. Secretaries, and other key officials are responsible for establishing an automated information systems security program that includes security training and awareness for all employees in accordance with VA policy and OPM regulations.

e. Facility directors are responsible for establishing AIS security and awareness training in their AIS security program as prescribed in VA Directive 6210 and VA organizational directives and procedures.

f. Managers and immediate supervisors are responsible for ensuring that all facility personnel attend formal AIS security and awareness training according to facility policy and procedures.

9. All VA employees, contractors, and other individuals using AIS resources are responsible for attending specifically assigned AIS security and awareness training.

4. **PROCEDURES**

a. Presented in this Chapter are training guidelines and requirements for computer security. Each organization should develop and issue specific guidelines for all users to effectively implement policy with regard to AIS security awareness and training within VA. The training should be designed to enhance employees' awareness of the threats to and vulnerability of computer systems and encourage the use of improved security practices. Due to the sensitive nature of certain positions, VA organizations should ensure that personnel in positions designated as "security officer, system administrator and in contractor positions" receive the appropriate AIS security training.

b. The VA standard for developing and conducting AIS security awareness and training for VA employees shall be the National Institute of Standards and Technology's (NIST) Special Publication 500-172, Computer Security Training Guidelines, and OMB Circular A-130, Appendix III, dated Feb. 8, 1996.

c. Personnel making use of automated information systems shall be aware of the vulnerabilities of such systems and trained in techniques to enhance security. Employees shall complete an initial AI.2 security training session prior to gaining access to a VA automated information system. This training may be held as part of orientation that new employees normally attend. Attendance shall be documented and placed in their official personnel file. Each administration and staff office is responsible for developing, implementing and maintaining a structured security program to include application security, personnel security, facility security and security awareness and training.

d. In compliance with 5 CFR, Part 930, Training Requirement for the Computer Security Act, all VA employees, including contractors, are to receive initial security training at orientation, and shall receive annual training in the following five content areas:

(1) Computer Security Basics. An introduction to the basic concepts of computer security practices and the importance of the need to protect the information from vulnerabilities to known threats.

(2) Security Planning and Management. Training which focuses on the policy level issues of AIS security and involves decision-making on the organization of the security program, security planning, and risk management process.

(3) Computer Security Policy and Procedures. Training which examines government-wide and Department specific security practices in the areas of physical, personnel, software, communications, data, and administrative security.

(4) Contingency Planning. Training covers the concepts of all aspects of contingency planning, including emergency response plans, backup plans and recovery plans. It identifies the roles and responsibilities of all employees involved.

(5) System Life Cycle Management. Training explains how security is addressed during each phase of a systems life cycle, which consists of system design, development, test and evaluation, implementation and maintenance. It also addresses procurement, certification, and accreditation.

e. VA employee training is divided into the following categories:

(1) Executives. Those senior managers who are responsible for setting Department computer security policy, assigning responsibility for implementing the policy, determining acceptable levels of risk, and providing the resources and support for the computer security program.

(2) Program/Functional Managers. Those managers and supervisors who have a program or functional responsibility (not in computer security) within the Department. They have primary responsibility for the security of their data and are responsible for designating the sensitivity and criticality of data and processes, assessing the risks to the data, and identifying security requirements to the supporting data processing organization, physical security staff, physical facilities personnel, and users of their data. Functional managers are responsible for assuring the adequacy of all contingency plans relating to the safety and availability of their data.

(3) **IRM, Security and Audit Personnel.** Personnel involved with the day-to-day management of the Department's information resources, including the accuracy, availability, and safety of these resources. Each organization assigns responsibility differently, but as a group these persons issue procedures, guidelines, and standards to implement the Departmental or component policy for information security to monitor its effectiveness and efficiency. They provide technical assistance to users, functional managers, and to the data processing organization in such areas as risk assessment and available security products and technologies. They review and evaluate the functional and program groups' performance in information security.

(4) AIS Management, Operations and Programming Staff. Personnel involved with the daily management and operations of the automated data processing services. They provide for the protection of data in their custody and identify to the data owners what those security measures are. The group includes: computer operators, schedulers, tape librarians, database administrators, and systems and applications developers. They provide the technical expertise for implementing security-related controls within the automated environment, and have primary responsibility for all aspects of contingency planning.

(5) (End) Users. Any employee or other customer who has access to a Department computer system that processes sensitive or non-sensitive information. This is the largest and most heterogeneous group of employees. It consists of everyone from the data entry clerk who has a personal computer with sensitive information to the executive.

f. These groupings are based on the need for employees within a given category to know or be able to perform the same or similar types of tasks. Each organization will determine specific training needs and categories to ensure that each employee within their organization receives the appropriate training.

g* Required Levels of Training. The level of training required in each training or subject matter area will vary from general awareness training to specific courses in such areas as contingency planning, depending upon the training objectives established by the Departmental components.

(1) Awareness Training. Awareness training should create the sensitivity to threats and vulnerabilities of computer systems and the recognition of the need to protect data, information, and the means of processing them. Initial security training shall cover rules of the system(s) to which the employee or contractor has access to; is consistent with guidance issued by NIST and OMB. Each VA employee or contractor shall receive initial AIS security training and thereafter receive "refresher" training on an annual basis.

(2) Performance Training. Employees develop skills to design, execute, or evaluate Department computer security procedures and practices. The purpose of this training is to enable employees to apply security concepts while performing the tasks that relate to their particular positions. It may require education in basic principles and training in state-of-the-art applications.

(3) **Policy-level Training.** Training provided for executives to enable them to understand computer security principles so that they can make informed policy decisions about the computer security program.

(4) **Implementation Training.** Training which provides program/functional managers with the ability to recognize and assess threats and vulnerabilities to automated information resources. These managers then are able to set security requirements which implement VA security policy.

5. REFERENCES

a. FPM Bulletin No. 410-131, 5 CFR Part 930 "Training Requirement for the Computer Security Act."

b. NIST Computer Security Training Guidelines, Special Publication 500-172 (Nov. 1989).

CHAPTER 3. SECURITY INCIDENT REPORTING PROCEDURES

1. PURPOSE and SCOPE

a. This Chapter establishes mandatory procedures for Automated Information Systems (AIS) security incident reporting within the Department of Veterans Affairs (VA). It is designed to provide Department-wide guidance to VA Administrations, staff offices, and other key officials on the proper response to and efficient and timely reporting of computer security related incidents, such as computer viruses, unauthorized user activity, and suspected compromise of VA data. These procedures are intended to meet required mandates of the Department and to assist in the protection of VA AIS resources from unauthorized access, disclosure, modification, destruction, or misuse.

b. An AIS security incident reporting system is necessary to identify a violation or incident, assess damage as a consequence of a violation, record the violation or incident, report the incident, and to use information to prevent the occurrence or violations. The reporting process outlined in these procedures are intended to discover and respond to AIS security incidents as they occur, will assist in preventing future incidents through awareness and, when combined with existing AIS security procedures, will augment VA AIS security controls.

c. These procedures apply throughcut the Department and to the security of VA resources, including AIS, data stored and processed on those AIS, data communication transmission media, and personnel who use VA AIS.

2. RESPONSIBILITIES

a. The Secretary of Veterans Affairs is responsible for administering VA security and ensuring a VA AIS security program is implemented.

b. The VA CIO, as delegated by the Secretary of Veterans Affairs, is responsible for ensuring that AIS security incident reporting is included in VA's AIS security program.

c. Deputy Assistant Secretary for Information Resources Management is responsible for:

(1) Overseeing and ensuring that VA AIS Security Program requirements and practices are implemented for all VA automated information resources through the Information Resources Security Officer (IRSO) for VA.

(2) Ensuring that VA AIS Security Incident Reporting policy is developed and issued.

(3) Reporting to and advising the Secretary and Deputy Secretary on major AIS security incidents affecting VA.

d. The Information Resources Security Officer for VA is responsible for:

(1) Ensuring that appropriate Department procedures conform to the requirements of the Computer Security Act of 1987 and yearly OMB bulletins regarding its implementation, OMB Circular A-130 and its appendices, other Federal laws and regulations, and promulgating such additional regulations and guidance as necessary.

(2) Serving as primary point-of-ccntact for VA and Government-wide AIS security matters affecting VA, and specifically, major AIS security incidents.

(3) Developing and issuing Departmental AIS Security Incident Reporting policy for VA.

(4) Providing assistance to Administration Heads, Assistant Secretaries, and other key officials in preparing their AIS Security Incident Reporting policy, procedures, and standards to comply with Departmental policy.

(5) Monitoring, reviewing, and evaluating compliance with AIS Security Incident Reporting procedures and tracking major AIS incidents annually.

(6) Reporting and advising the Deputy Assistant Secretary for Information Resources Management on major AIS security incidents.

(7) Establishing an Incident Reporting and Response Capability in the Department to assist VA Administrations and staff offices by:

(a) Identifying causes for AIS security violations/incidents.

(b) Recommending corrective measures and solutions to resolve incidents.

(c) Coordinating information exchange of VA AIS security violations and incidents with Computer Emergency Response Team (CERT) organizations.

e. The Inspector General is responsible for:

(1) Investigating and auditing major AIS security incidents when appropriate, and conducting criminal investigations, as warranted.

(2) Providing advice on coordinating an investigative process for AIS security inc dents and reconciliation of those incidents.

f. The General Counsel is responsible for:

(1) Interpreting laws, regulations;, and directives applicable to VA AIS security activities, and specific to AIS incident occurrences and reporting of those occurrences.

(2) Rendering legal advice and other legal services with respect to AIS security incidents upon request to Administration heads, Assistant Secretaries, and other key officials.

g- Administration Heads, Assistant.. Secretaries, and other key officials are responsible for:

(1) Ensuring their Administration or staff office comply with the requirements of the VA AIS Security Incident Reporting policy.

(2) Ensuring that policy, procedures, and standards which meet the requirements of the VA AIS Security Incident Reporting procedures are developed for their respective Administration or staff office.

(3) Ensuring that their Administration or staff office Information Security Officer (ISO) identifies and reports major AIS security violations of AIS security policies, procedures, and accepted pramctices to the VA IRSO.

(4) Creating an incident response capability within their automated information system security program.

h. Each Facility Director is responsible for:

(1) Implementing the AIS security requirements of the ir respective faci lity.

(2) Ensuring that the facility IS0 investigates, reviews and records AIS security incidents at the facility and reports the incidents to the appropriate Administration or staff office ISO.

(3) Ensuring that the assigned Incident Response team is notified when a reportable incident occurs.

i. The facility IS0 is responsible for:

(1) Establishing the facility's AIS security incidents reporting system.

(2) **Logging,** investigating, and reviewing AIS security incidents at the facility and reporting the incidents to the appropriate Administration or staff office ISO.

(3) Establishing contact with the <assigned Incident Response team when a reportable incident occurs.

j- Managers and Supervisors are responsible for:

(1) Implementing the requirements of their respective Administration or staff office Information Security Officer AIS Security Incident Reporting procedures within their assigned areas of management control.

(2) Ensuring that AIS security violations/incidents occurring within their assigned area of management control are reported to the appropriate facility ISO.

(3) Ensuring on a regular basis that all assigned employees, contractors and other individuals, who develop, operate, administer, maintain, or use VA AIS, understand they are responsible for reporting actual or suspected AIS security incidents to their immediate supervisor or facility ISO.

k. All VA employees, contractors, and other individuals with access to sensitive areas or automated information systems are responsible for reporting AIS security violations or incidents to their supervisor or ISO.

3. PROCEDURES - AIS SECURITY INCIDENT REPORTING SYSTEM

a. Security Incident Standards

(1) Computer security incidents can range from a single virus occurrence to a hacker attacking many networked systems, or such things as unauthorized access to sensitive data and loss of mission-critical data. An incident refers to a computer security problem arising from a threat,.

(2) AIS security incidents to be reported and tracked can be categorized as follows (these types of acts are not all-inclusive):

(a) Circumvention of AIS security controls, safeguards and/or procedures;

(b) Unauthorized access, use, disclosure, alteration, manipulation, destruction, or other misuse of data and AIS;

(c) Theft, fraud, or other criminal activity committed with the aide of AIS resources;

(d) Theft, loss or vandalism of AIS hardware, software or f irmware;

(e) Issues affecting confidentiality, integrity and availability of data and AIS; and

(f) Unauthorized downloading or copying of VA sensitive information.

(3) Examples of specific reportable incidents which can be reported under the six categories of incidents include (but are not limited to):

(a) Unauthorized access to or use of sensitive data for illegal purposes;

(b) Unauthorized altering of data, programs, and AIS hardware;

(c) Loss of mission-critical data, i.e. patient, financial, benefits, legal, etc.;

(d) Environmental damage/disaster (greater than $10,000) causing loss of AIS services or data, or which may be less than $10,000 in damage yet have affected the Administration's or staff office's capabilities to continue day-to-day functions and operations;

(e) Infection of sensitive systems or software by malicious code, i.e. virus, Trojan Horse, etc.;

(f) AIS perpetrated theft,fraud and other criminal computer activity;

(g) Telecommunications/network security violations, i.e., networks (including local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs)) which experience service interruptions that cause an impact to an indefinite number of end users;

(h) Theft or vandalism of AIS hardware, software or firmware whose loss did or may affect the organization's capabilities to continue day-to-day functions and operations;

(i) Unauthorized access to data when in transmission over communications media;

(j) Loss of system availability impacting the ability of users to perform the functions required to carry out day-to--day responsibilities; and

(k) Unauthorized access to and/or unauthorized use of the Internet.

(4) VA Administrations and staff offices shall require their subordinate offices and facilities to report AIS security incidents, which the organization interprets as damaging to the organization's mission, to VA Administration or staff office ISO.

(5) VA Administration's or the staff office's IS0 shall report those incidents which the organization interprets as damaging to the organization's mission, to the VA's OIRM Information Resources Security Officer (VA IRSO).

b. Reporting Procedures

AIS security incidents as defined in paragraph 3-a.(2) will be reported by the person observing or discovering the occurrence to the facility ISO. The facility IS0 is responsible for recording and reporting security incidents to the Administration or staff office IS0 for tracking and reconciliation of the suspected incident. Suspected AIS security incidents will be reported to ISOs within 48 hours of the occurrence. Additionally, those incidents which are determined to affect an Administration or staff offices' capability to accomplish critical functions, restrict the availability of a system or communications medium, i.e. LAN, MAN, WAN, network, etc., or result in a monetary impact to the Administration or staff office, will be reported within 48 hours of the occurrence to the VA IRSO, located in the Office of Information Resources Management, by the Administration or staff office ISO.

(2) AIS security incidents shall be recorded on a security incident form or log as defined by the facility. Essential information about the security incident should be identified in as much detail as possible, at the time of occurrence. Some information may need to be added at a later time based on the investigation/closure of the incident. The followinq minimum information about a security violation or incident shall be entered on the AIS security violation/incident form:

(a) Location of incident and organization filing report;

(b) Reported by (Name, Title and Crganization);

(c) Date and time of report filing;

(d) Date and time of incident;

(e) Details of incident (include names of personnel involved and description of the who, what, when, where, how, and why):

(f) The name and title of the person to whom the incident initially was reported to;

(g) Identification of whether the Inspector General or appropriate law enforcement organization has been notified;

(h) Incident impact on day-to-day operations;

(i) Action taken to contain the incident and resources required to correct the incident (in cases of system outage note what vendors have been contacted);

(j) Short-range corrective action, such as discontinuing the use of an infected computer diskette, immediately removing a terminated employee's access privileges;

(k) Long-range corrective actions, as necessary;

(1) Estimated monetary damage; and

(m) Additional information, as appropriate

(3) The information collected on the AIS security incident form shall be reported to the Administration or staff office IS0 in a confidential manner, which may include the following methods. Initial reports of serious incidents or violations may be reported by telephone. Reports may be sent by U.S. mail using the double-envelope method, couriers, or secure facsimile. Follow-up contact will be established with the reporting facility or office by the Administration or staff office IS0 , and tracking for each incident will be continued until final closure. Each facility, local or office level ISO, or manager/supervisor will be responsible for making the determination of whether the AIS security incident at their level is reportable based on the definitions provided in this procedure and ensuring that reports are filed with their respective Administration or staff office ISO.

(4) Significant AIS security incidents shall be reported first to assigned VA Incident Response and Security Team which will identify and assist in resolving reported incidents.

c. Protection of Report Information. AIS security incident report information will be treated as sensitive information and safeguarded as equivalent to Privacy Act information, at a minimum. Access to AIS security incident information should be restricted and shall be stored in locked areas.

d. **Tracking of AIS Security Incidents**

(1) Each VA Administration or staff office IS0 is responsible for tracking AIS security violations and incidents for their organization. Tracking will include monitoring each incident through final closure and maintaining a copy of the incident report for a period of three :3) years. Reports of security violations and incidents shall be prepared and maintained by the Administration or staff office ISO. Those security violations and incidents which threaten critical organization functions shall be reported within 48 hours to the office of the VA IRS0 by the Administration or staff office ISO.

(2) The office of the VA IRS0 shall advise the DAS/IRM of security violations and incidents reported from VA Administration or staff offices which threaten critical VA functions.

e. **IRS0 Handling of Reported AIS Security Violations and Incidents**

(1) The VA IRS0 shall establish a log of reported security incidents. Automated files of reported incidents shall be protected against unauthorized access and not accessible through a network.

(2) Major elements of security incident records created and maintained by the VA IRS0 shall include: name of VA Administration or staff office making the report; number of violations and incidents by type or nature, total number of violations and incidents; number of unresolved violations and incidents; and the estimated monetary loss attributable to all reported incidents.

f. **Reporting of Security Incidents, and Violations to the Media.** All VA components shall refer questions from the media (e.g., newspapers, television, and radio) concerning AIS security violations or incidents to VA's Office of Public Affairs in VACO. The Department will respond to media requests for records concerning security under the Freedom of Information Act (FOIA) in accordance with VA procedures for responding to FOIA requests rather than with the procedures specified here.

4. **REFERENCES**

a. Information Resources Security Handbook, Office of Information Resources Management, H-003-1, 1991.

b. National Institute of Standards and Technology (NIST), NIST Special Publication 800-3, Establishing a Computer Security Incident Response Capability (CSIRC), November 1991.

c. Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems, dated February 8, 1996.

CHAPTER 4. VIRUS CONTROL PROCEDURES

1. **PURPOSE.** The following components provide prevention, detection, identification and recovery from computer viruses. This handbook contains mandatory Department of Veterans Affairs (VA) procedures for:

a. Reducing VA vulnerability of VA personal computers, local/wide area networks (LAN/WAN) from the threat of computer viruses and other forms of malicious code.

b. Ensuring timely detection of computer virus infections.

c. Providing a reliable means for containing and eliminating infections when they do occur.

2. **BACKGROUND.** The following includes basic background information necessary for a basic understanding of the computer virus threat:

a. What is a computer virus? A computer virus is a malicious software program with the ability to replicate itself, thereby spreading from computer to computer. The result of this infestation may simply be annoying, such as a display of messages or minor degradation of system performance. Viruses can also have catastrophic consequences, such as the complete destruction of all programs and data stored on a system's hard disks. Damages may not be limited to individual computers as accessible network disk drives may be infected and become a standing source of infection for other connected computers. Viruses may modify or destroy data rendering systems and possibly entire networks unusable. For the sake of simplicity in this document, any type of malicious program code will be referred to as a virus.

b. There are four types of viruses: The boot sector infector, the file infector, the companion virus and the Macro virus. Some viruses fit into more than one category because they infect boot sectors and files and so are called multipartite viruses. Some of these viruses may try to hide themselves by taking control of the operating system; these viruses are called stealth viruses. Some viruses encrypt themselves so every infection appears to be different; these are called encrypted viruses.

(1) The Boot Virus. The boot sector virus writes itself into the DOS system area on the floppy disks and hard disk:; it infects. This type of virus accounts for over 70% of all reported virus infections. It can only be passed to your computer when you inadvertently attempt to boot from a floppy disk left in the disk drive (generally people boot their computers from the hard drive). Once the computer's hard disk has become infected, the computer becomes a source for spreading the virus. The virus becomes active each time the system boots up and writes itself out to every floppy that passes through your computer. The boot virus cannot infect a network and cannot be passed throughout the organization through the LAN.

(2) The File Virus. The file virus or program virus, as it is often called, infects program files by attaching themselves to them or overwriting a portion of the program with the virus code. These viruses are easily passed over LAN/WANs or any other network, including Internet. They can be sent as attachments to e-mail or placed on electronic bulletin boards for the unsuspecting to download. They become active when the program they are attached to is executed.

(3) The Companion Virus. The companion virus may exist as a duplicate file but have the COM extension instead of the EXE extension. The COM companion virus executes first and after becoming active, it passes control back to the EXE which executes normally. There is also a type of companion virus that modifies the pointers in the directory to point to a virus instead of the intended program. When a user attempts to execute a program, the virus executes and after becoming active, it executes the program that the computer user actually was trying to execute.

(4) The Macro Virus. Many software products include macro programming languages or tools allowing users the ability to automate tasks that were once repetitive. Due to the continual enhancements developers have made to these macro languages many are now sophisticated enough to create malicious programs which technically are computer viruses. Macro viruses can replicate and spread from computer to computer so they technically fall into the realm of the computer virus.

c. There are three main components to the logic code of a virus: the replication logic, trigger logic, and the attack or bomb logic. The replication logic is the portion of code that allows the virus to replicate itself; the trigger logic decides whether to attack or go dormant (replicate but not attack); and the attack logic destroys data or could be a relatively benign taunting message.

d. Other Forms of Malicious Programs. Though not covered specifically, many of the procedures described within this Chapter are equally applicable to other forms of malicious program code.

3. RESPONSIBILITIES

a. The Department IR Security Officer (IRSO) will:

(1) Manage the VA Computer Virus Protection Program. Collect AIS security violation and incidents information consistent with VA AIS Security Incident Reporting policy (Chapter 3, VA Handbook 6210). Maintain reports of incidents and share information on detection and removal of acute infections.

(2) Establish and disseminate virus protection procedures and guidelines to VA organizations on the prevention, detection, and removal of computer viruses.

(3) Serve as the Department point-of-contact for virus-related issues, including information on reputable anti-virus software and the identity of local VA office AIS security representatives.

(4) Provide Department-wide technical assistance in response to virus incidents, by recommending anti-virus software or other methods of detection and removal.

(5) Consult with automation personnel and VA network administrators (those having the responsibility of managing or maintaining a PC-based network) regarding virus prevention, detection and identification, and recovery procedures.

(6) Conduct reviews as necessary to ensure compliance with the mandatory security program requirements.

b. **All VA offices shall:**

(1) Establish operational procedures for network system administrators to implement an effective virus protection program.

(2) Assist the Department IRSO in responding to virus incidents.

(3) Contribute to the free flow of information concerning viruses by reporting incidents to the Department IRSO.

(4) Assist the Department IRSO in compliance reviews of the virus program.

(5) Ensure that maintenance contracts with consultants, repair technicians and troubleshooters contain security requirements for non-VA employees to follow, and includes security measures, such as virus scanning and prevention techniques.

c. VA Network System Administrators will:

(1) Where a network utility, facility, or mechanism exists, restrict network users so they cannot write to program files on network drives. Installed programs are never written to and so should be set as "read only or execute only." When possible,access controls should be set to prevent even network administrators from being able to write to program files (though they should have "delete" privileges). Doing this will prevent computer viruses from attaching to program files that are shared by all.

(2) Follow virus protection, detection and identification, and recovery policies and procedures. Maintain a current copy of licensed virus protection software on bootable write-protected diskettes.

(3) Use system administrator privilege on a LAN or a WAN only when doing administration or maintenance of the network requiring such higher levels of privilege. When assisting customers, privileged users should not log onto the network as system administrator from any machine that has not first been determined to be virus-free. For routine work, such as e-mail, word processing, etc., administrators shall use accounts with normal user privileges.

(4) Keep write-protected copies of original software loaded to network servers to perform a necessary restore to workstations and to do regular back-ups of critical server data.

(5) Comply with directives provided by the Department IRS0 in response to specific virus incidents, where applicable.

(6) Prepare additional local direction, such as operating memoranda, policies and procedures, where applicable.

(7) Report all computer virus incidents to the facility Director or designee and the facility ISO, and notify all network users.

d. **VA computer users will:**

(1) Employ physical access protection for all Department microcomputers to restrict access by unauthorized person..;. Unknown and potentially unauthorized persons will be challenged in regard to their authorization to use equipment.

(2) Ensure that software loaded or data disks used on their computer are first scanned for possible viruses.

(3) Perform regular back-ups of computer data files. The frequency of these back-ups should be commensurate with the nature and criticality of the data stored.

(4) Use current anti-virus software on a daily basis for any microcomputer used in processing sensitive or critical VA information, including:

(a) portable microcomputers;

(b) microcomputers used to process diskettes received from sources outside VA;

(c) microcomputers returned from outside repair facilities;

(d) microcomputers that have had diagnostic utilities or other software run on them by repair technicians;

(e) employee-owned microcomputers that are used to process VA information (whether at home or office); and

(f) sales demonstration disks and beta test versions of software.

(5) Use anti-virus software to scan the entire hard disk after files have been recovered from back-ups if the recovery was required due to a virus-related incident.

(6) Use only software proven to be virus free after scan testing. Refrain from using unsolicited software sent to you by mail or obtained from external sources until tested.

(7) Obtain "shareware" software directly from official sources such as the developers' electronic bulletin board systems (BBS).

(8) Use only one write-protected boot disk for each floppy-based microcomputer and control access to this disk. On systems with hard disks, ensure the system boots from the hard disk and no floppy has been inadvertently left in the floppy drive (the computer may attempt to boot from it). If possible, configure the computer to boot only from the hard disk.

(9) Ensure original manufacturer software is securely stored in the event that programs must be restored to disk. Data can be backed up and software retained on original diskettes as back-ups.

(10) Comply with additional direction by the Department IRS0 and organization AIS security representatives in response to specific virus threats, where applicable.

(11) Report all computer virus incidents to the facility or organization IS0

e. Consultants, Repair Technicians and Troubleshooters will:

(1) Employ a reputable and current anti-virus product and scan all operating PCs before beginning to work.

(2) Report all computer virus incidents to their organization ISO.

4. PROCEDURES. While current physical and logical access controls provide protection against unauthorized system access on many networked computers, an authorized user may unknowingly introduce virus-infected software locally through floppy drives or remotely via a modem. A single infected microcomputer on a network can rapidly infect every workstation and server on that network. Implementation of the measures prescribed in this chapter will provide reasonable protection of VA information resources against the threat of computer viruses.

a. **FIRMR** (Federal Information Resource Management Regulations). VA must continue to develop an environment that will minimize the risks and consequences of virus infection to computers and LAN/WANs and is bound by the FIRMR Bulletin C-28, "Computer Viruses."

b. **Physical Access Control.** Physical access control will be employed on all Department computers to restrict use to authorized persons. This means that computers should be physically secured to prevent access by an unauthorized person.

c. Key Locked. Every newer personal computer has a key lock though it should be noted that this may only give an extremely low level of security. If keys are used as a first line of defense, then the supervisor or other individual should keep the backup key in the event that the organization needs access to that computer.

d. **CMOS Security.** Many PCs have a CMOS setup routine that can be accessed from DOS by hitting the correct key combination. On many PCs the key combination is Ctrl-Alt-Esc, but your PC may be different. Before you attempt to change your PC's CMOS setup, see your owners manual for the key combination for your PC. Once you bring up the CMOS setup routine you can password protect your CMOS so it cannot be changed without the password, and you can password protect your PC so that it will not boot without the password. This gives you a low level of access control to your PC and may help to keep unauthorized persons from using your PC. In the same CMOS routine you should also set your PC to force booting from only the C: drive (hard disk). This will eliminate the possibility of your ever getting a boot virus, as it makes it impossible for your PC to boot from an infected floppy.

e. **Backups.** If anti-virus software efforts fail you will always be able to resume business as usual if a reliable backup has been done. Regular and frequent back-ups of computer data files should be performed to aid in the recovery from a virus or any data loss situation. Of course, if the system has been unknowingly infected by a virus for sometime, backups may be infected. When backups are infected, generally only the program files will be infected - not the data. In order to restore the program files to their original state, the user should be able to fall back to the original manufacturer's software diskettes. These should have been write-protected prior to installation (when possible) and stored securely for use in restoring original program file:;. In some cases where a mirror image of a complete disk is taken as a backup, a boot virus can be transferred to the backup. Restoring from such an infected backup will certainly restore the virus. For this reason, it is important to do file-by-file type backups rather than the "mirror" image or complete back-up.

f. **Virus Scanning.**

(1) When personal computers are attached to a LAN, they should contact the LAN System Administrator about having anti-virus software installed to secure each workstation against computer viruses. The LAN Administrator will monitor the LAN servers for virus activity through the use of anti-virus software. Set up the anti-virus software so that it scans the PC automatically when it is booted. Anti-virus software will be used on all local area networks (LAN) and connected workstations. Workstations to be connected should be determined to be virus-free before connection. There are anti-virus products that will check the boot area of the disk on boot up and may even restore the correct boot area if a virus has infected it. There are resident monitors that run continuously in the background. These should be used whenever possible because they prevent the admittance of viruses during the workday (after the initial. scan has been done). However, in some instances, shortages of system memory may preclude the use of a resident scanner.

(2) An office may be using a variety of anti-virus software, possibly different products from what are used on the LAN or elsewhere. There is strength in diversity. No single anti-virus product can detect every virus, so the fact that you are using an additional product may help to identify a virus that may otherwise go undetected. Special consideration should be given to the purchase of products that do not rely strictly on signature scanning as the primary method of detecting viruses. Signature scanners must be continually updated with the signatures of new computer viruses and may not be able to detect many encrypted viruses. Many products now use signature scanning merely as a method of identifying a computer virus once detected. It is highly recommended that'a product be chosen that uses one of the following methods of detection: Generic Differential Detection, Holistic scanning, Heuristics or another non-signature based method, as the primary detection method.

g. **Scan Incoming Software.** Software obtained from external sources should be used only after it has been "scanned" by a reputable and reasonably current anti-virus product. All PCs and servers should undergo regularly scheduled scanning. Public domain "shareware," as well as commercial software, will be "scanned" for viruses before use. Computers returned from outside repair facilities will be "scanned" for viruses before being attached to a network or put into operation. Software utilities used by repair technicians will also be "scanned" before use. Repair/troubleshooting technicians should scan their software before use and keep it write protected while in use.

h. VA Developed Software. Software produced within VA will be designed to prevent it from being an avenue for infection, where possible. Developers may choose to write program routines that incorporate integrity checking algorithms or encryption for the program itself. All program disks should be "scanned" using a reputable and reasonably current anti-virus product before distribution. Only write-protected diskettes should be distributed.

ı. **Diskettes from Home.** Diskettes taken home and used on home computers or brought from any non-VA location should be "scanned" with a reputable and reasonably current anti-virus product before use on a VA computer. Many home PCs are infected due to downloading anonymous software from electronic bulletin boards, trading games, etc. It is easy for a PC to become infected with a virus under these circumstances. If diskettes are taken home to do work, then they should use the same good security practices at home as at work. However, scanning the disk for viruses after returning to work is a good preventive measure.

j. Trophy Viruses. Unless you are a member of an AIS Security staff and need to save computer viruses for study and distribution to anti-virus community, do not attempt to save them. However, an infected file or disk can be retained for the purpose of supplying the anti-virus software developer with the virus for analysis. This diskette should be clearly marked as infected and sealed in an envelope so that it is not inadvertently used. Other than these exceptions, when a virus is detected, it should be destroyed immediately.

5. **REFERENCES**

a. For Your Eyes Only, quarterly AIS security bulletin for the Department of Veterans Affairs, Library of Congress serial publication number ISSA 1071-4286.

b. National Institute of Standards and Technology (NIST) Special Publication 500-166 Computer Viruses and Related Threats: A Management Guide, by John P. Wack and Lisa J. Carnahan.

CHAPTER 5. COPYRIGHT SECURITY PROCEDURES

1. PURPOSE AND SCOPE

a. All VA employees are required to protect government and public interests as they perform their duties. This includes assuring that government-acquired software protected under the Copyright Act is used in accordance with the law and the software licensing agreement. It is the responsibility of all VA organizations and employees to ensure that copyrighted software is licensed properly before being installed on VA equipment. Title 17, United States Code, Section 106, gives copyright owners exclusive rights to reproduce and distribute their material; Section 504 states that copyright infringers can be held liable for damages to the copyright owner. Title 18, United States Code provides felony penalties for software copyright infringement. This policy does not apply to software developed by the Department or for use by the Department under a Departmentwide license.

b. Special purpose software shall be used to perform a software audit which will inventory and document software on each PC in the organization. Such software may be a commercial product or may be acquired free from the Software Publishers Association (SPA) through the organization's Information Security Officer (ISO).

c. Individual employees may not install privately-owned software on government equipment unless it is in the best interest of VA. Authorization and justification for the installation of privately-owned software must be approved, in writing, by the VA employee's facility or organization management. Prior to authorization, the employee's management should require the employee to provide the software license and give assurance that copyright infringement will not result from the installation, in addition to other local management requirements. Individuals not following these procedures may be held personally liable for any violations of the copyright law and subject to the penalties specified in Titles 17 and 18 of the United States Code.

d. The Computer Software Rental Amendments Act of 1990 (Title VII.1 Public Law 101-650) prohibits the rental, leasing, or lending of original copies of any computer program for the purposes of direct or indirect commercial advantage without express permission of the copyright owner.

e. Old versions of software that have been upgraded shall be disposed of in accordance with the licensing agreement and may have to be returned to the manufacturer or destroyed, depending on the software licensing agreement terms. The new upgrade is usually intended to replace the old software, resulting in a single copy license. It may be a violation of copyright to continue to operate old versions after the upgrade has been installed. VA facility management shall ensure that software licensing agreements permit old versions of software that have been upgraded, to be loaned or taken home by VA employees. This practice will avoid violating the copyright law.

2. RESPONSIBILITIES

a. Each facility director is responsible for ensuring that software copyright procedures are included in the facility's AIS security program and are complied with.

b. Managers and immediate supervisors are responsible for ensuring that employees are trained in and follow the established procedures and acceptable practices allowed under software copyright laws and VA facility policy and procedures.

c. The facility ISO, for the Director, implements the facility's AIS security program and its components, and ensure:; the facility security program is in compliance with software copyright laws and VA facility and Central Office policies.

d. All VA employees, contractors, and other individuals using IRM technology resources, shall adhere to software copyright laws and VA facility security policy and procedures.

3. PROCEDURES. The following practices and procedures will be adhered to by all employees. VA managers and supervisors will be held accountable for conducting periodic audits to ensure compliance:

a. Install on VA systems only commercial software, including shareware, that has been purchased through the government procurement process. An exception to this rule is when privately-owned software is authorized to be installed on government equipment by VA facility or organization management.

b. Follow all provisions of the licensing agreements issued with the software and register organizational ownership.

c. Make only authorized copies of copyrighted software. Normally, the license will allow a single copy to be made for archival purposes. If the license is for multiple users, the authorized number of copies shall not be exceeded.

d. At least annually, inventory and maintain written records of all software on each individual PC. This inventory shall be compared with the organization's licensing agreement records to ensure licensing compliance.

e. Maintain written records of software installed on each machine and ensure that a license or other proof of ownership is on file for each piece of software.

f. Store licenses, software manuals and procurement documentation in a secure location (e.g., locked file cabinet, etc.).

g. When an upgrade to software is purchased, dispose of the old version in accordance with the licensing agreement. Upgraded software is considered a continuation of the original license, not an additional one. The continual use or redistribution of old versions (that have been upgraded) may be a violation of copyright law.

h. Some government-owned software licenses allow employees to take copies home for use on their privately-owned computers under specific circumstances (e.g., for government work, but not personal business). Unless the license allows this specifically, doing so is in violation of the copyright law, and the individual may be held liable.

i. All unauthorized copies of software, identified during audits or compliance reviews, shall be removed immediately.

4. REFERENCES

a. P.L. 102-561, Amendment to Title 18, Criminal Penalties for Copyright Infringement.

b. P.L. 101-650, The Computer Software Rental Amendments Act of 1990.

c. Title 17, U.S.C, Copyright Act.

CHAPTER 6. PROCEDURES FOR SAFEGUARDING SENSITIVE INFORMATION STORED ON AUTOMATIC DATA PROCESSING EQUIPMENT DURING DISPOSAL

1. PURPOSE AND SCOPE. This Chapter provides the authority, responsibilities, procedures and controls required for removing sensitive information that resides on automatic data processing equipment (ADPE) storage media prior to its disposal. The provisions of VA Directives 6300 and 6210 govern the protection and disclosure of sensitive information in VA. Sensitive information must always be protected from unauthorized access and disclosure. Inadvertent disclosure of sensitive information can occur when the storage media for this information is released for disposal without the permanent erasure of the sensitive information. The residual physical representation of data on storage media is known as data remanence. This Chapter provides the appropriate procedures, safeguards, and actions to be taken to protect sensitive information before the storage media containing the sensitive information is released for disposal. The provisions of this Chapter and governing directive are applicable to all organizational elements within the VA and must be implemented at all VA offices and facilities within 180 days from the date of issuance.

2. RESPONSIBILITIES

a. The VA CIO is responsible for developing and recommending policies and controls for the selection and protection of sensitive information in the Department.

b. Administration heads, Assistant Secretaries, Deputy Assistant Secretaries and other key officials are responsible for ensuring that offices and facilities under their control include policy and procedures in their computer security programs for the protection of sensitive information during the disposal of ADPE storage media.

c. Each facility director, manager or other person accountable for the control of ADPE is responsible for the development and implementation of rules and procedures for safeguarding sensitive information contained on storage media before it is disposed of.

d. The VA Information Resources Security Officer (IRSO) is responsible for monitoring, reviewing and evaluating compliance with this automated information system (AIS) security program directive. The IRS0 reports the results of reviews to the Deputy Assistant Secretary for IRM.

3. PROCEDURES

a. This Chapter provides the procedures and methods to apply when ADPE with permanent storage capabilities (retention of data occurs in storage, on either removable or "non removable" media), including magnetic, solid-state and optical storage media, is being released for disposal. This Chapter only applies to the removal of sensitive information from ADPE slated for disposal, not the disposal of the ADPE. The disposal of ADPE must comply with the FIRMR Part 201-23, Disposition, and the applicable VA policies. The term disposal, as used in this Chapter, applies to actions where equipment is excessed, transferred, discontinued from rental/lease, exchanged, or sold.

b. Mandatory Disposal Procedures. Procedures and standards governing the disposal of sensitive information must be developed and implemented by each facility director, manager or person accountable for the control of ADPE that processes or stores sensitive data in VA. Disposal procedures for storage media that meet these criteria are mandatory and shall include, as a minimum, the following methods, controls and practices:

(1) Operating Procedures. Written operating procedures which specify security requirements and standards for disposal of storage devices that contain sensitive information shall be used. Procedures for the removal or clearance of those media before release or reuse of the equipment is permitted shall also be included in the procedures. A quick reference guide detailing procedures for disposing of a personal computer is contained in Appendix A.

(2) Trained Staff Assigned. Staff trained in data eradication methods and procedures shall be used to irrevocably clear and remove sensitive information from equipment and storage media scheduled for disposal or release.

(3) Method for Cleaning Storage Media. The method selected for clearing/purging storage media must fit your situation, storage device to be cleared, the sensitivity of the data, the acceptable level of data remanence (how much data remains on the storage media) and the possible or potential risk of data recovery after the equipment is released. The principal methods for safeguarding sensitive information during the dispoaal or repair of equipment include: overwriting; degaussing; destruction of' the storage media; removal of the storage media; or declassification of the information.

(4) Approved Software. Only software adhering to the VA standard shall be used for overwriting and removing of sensitive information; overwrite software itself must be protected from unauthorized modification or use. The VA standard used for overwrite software is found in the National Computer Security Center's publication, A Guide to Understanding Data Remanence in Automated Information Systems, NCSC-TG-025 Version-Z.

(5) Approved Demagnetizing Device or Demagnetizing Services. Only manufacturer recommended degausser products that are listed for your hardware or storage media shall be used. Contracting with the appropriate vendor for this service may be an acceptable alternative to the purchase of equipment to demagnetize storage media. Where contracts with vendors already exist for services and maintenance of PCs, contact the VA project manager for that specific contract. An agreement for demagnetizing services may exist or could be centrally developed. When using contracted vendor services, specific measures, such as non-disclosure agreements with the vendor, must be devised and implemented to ensure that vendors or other personnel authorized to access sensitive data preserve the confidentiality of that data during the data clearance process..

(6) Sensitive Data Protected during Maintenance and Repair. Procedures shall be established by Department components to ensure that authorized personnel, including non-VA personnel, such as vendors and contractors, preserve the confidentiality of sensitive data and that unauthorized personnel do not access sensitive files during repair or maintenance. These procedures shall be consistent with statutes and existing policies which govern actions during maintenance and repair of ADPE.

(7) Equipment and Storage Devices Certified. An official at each station, facility and key VA Central Office organization shall be appointed to certify, in writing, that equipment with storage media has been properly cleared of all information before it is excessed, transferred, discontinued from rental/lease, exchanged, sold or otherwise released.

(8) Information Removed from Storage Media Properly Retained or Disposed of. Prior to disposal or release of the computer storage media, all records maintained on the storage media shall be retained or disposed of in accordance with the instructions in the approved records control schedule. The responsible records control office shall be contacted for guidance.

c. When maintenance or repair is required for ADP equipment with storage media or the storage media alone, sensitive data residing on that equipment must also be protected. Specification of procedures for the protection of sensitive information when maintenance or repair is planned is beyond the scope of this policy. Department components are expected to establish procedures to preserve the confidentiality of sensitive data under these circumstances consistent with any applicable statutes and existing directives.

d. When disposal of storage media involves transfer between or within VA facilities, these procedures are limited to instances where ADPE storage media containing sensitive information is sent to a VA facility or to a VA component within a VA facility where individuals with access do not have a need to know. "Need to know" is the principle that a Department official or employee may have access to sensitive information in VA computer systems and storage media only when the official or employee needs access to that information in order to perform an assigned task or duty within the official assigned responsibilities of the individual.

e. Security planning that includes mandatory disposal procedures will help prevent the compromise of sensitive information contained in a computer system or its parts after it is out of the control of the VA organization that had custody. Appendix A to this Handbook contains a list of steps for the removal of sensitive information from a personal computer before it is released.

f. Requirements established in this handbook for safeguarding sensitive information are in addition to requirements in other VA directives that govern the handling and disposition of FIP resources.

g. Sensitive information as used in this Chapter does not include computer software or computer programs that process sensitive information or other VA data.

4. REFERENCES

a. Computer Security Considerations in Federal Procurements, National Institute of Standards and Technology; Special Publication 800-4.

b. DOD Computer Security Center (NSA), A Guide To Understanding Data Remanence in Automated Information Systems, NCSC-TG-025 Version 2, September 1991.

c. DOD 5200.28 STD, "Trusted Computer System Evaluation Criteria," December 1985.

d. Privacy Act of 1974, 5 U.S.C. 552a.

Chapter 7. LOCAL AREA NETWORK SECURITY PROCEDURES

1. PURPOSE AND SCOPE. Local area networks (LANs) have become an important tool for organizations to meet their information processing, communications, and office automation needs. LANs provide the distribution of data, applications, and communications services to network members. By way of a common network operating system (NOS), LANs connect file servers, workstations, printers, and mass storage devices, and enable users to share resources and functionality. With the distribution of data over the LAN to the organization, security for the protection of data must also be distributed. It is important to understand the security needs before appropriate security procedures and measures can be devised and implemented.

2. RESPONSIBILITIES

a. Administration Heads, Assistant Secretaries, and other Key officials are responsible for ensuring development of LAN security policy and procedures in their organizations.

b. Each facility director is responsible for implementation of LAN policy and procedures.

c. Managers and immediate supervisors are responsible for informing staff about this policy, assuring that each affected person has access to a copy, and ensuring employees receive training on this aspect of AIS security.

d. LAN managers and administrators are responsible for implementing specific LAN security measures and techniques to protect PCs, network servers, and other network resources and comply with the facility's or organization's LAN security policy.

e. All VA employees, contractors, and other individuals using IRM resources are responsible for complying with security policy established by those primarily responsible for the security of the data, and for reporting to management any suspected breach of security.

3. PROCEDURES

a. **LAN Security Requirements**

Minimum essential security requirements for local area networks (LANs) in VA shall include:

(1) Define LAN configuration

(2) Determine the risks to the LAN: A risk assessment should be done to determine the criticality of the LAN based on the level of sensitivity of the information, the vulnerabilities and the safeguards to be taken to reduce those vulnerabilities.

(3) Select security measures: Determine security procedures and devices needed to secure the LAN at an acceptable level of risk.

(4) LAN information security policy.

(5) Maintenance of confidentiality of sensitive data as it is stored, processed or transmitted on a LAN.

(6) Maintain the integrity of data as it s stored, processed or transmitted on a LAN.

(7) Maintain the availability of data stored on a LAN, as well as the ability to process the data in a timely fashion.

b. **Components of Network Security Design**

Mandatory elements of a network system design shall include:

(1) LAN Configuration description. LANs should be configured to limit each user's access to only the resources they need to accomplish their job.

(2) Develop LAN security requirements.

(3) Implement and test security measures. Unauthorized LAN Access:

(a) List possible vulnerabilities, such as lack of or insufficient identification and authorization process, improper password management, etc

(b) Computer users shall be required to have a separate ID and passwords. Users shall be required to change their passwords at least once every six months, password length must be at least six characters in length, and are not an English word or name.

(c) The LAN must have an intruder lock out feature that would suspend an account after three invalid attempts to logon. This will help the systems administrator determine if efforts are being made to compromise LAN security. This limits the number of failed login attempts before suspending that account ID. When a lock out occurs, the systems administrator should investigate to determine whether the action was that of an authorized user or an attempt to intrude. Attempted intrusions should be studied for ways to improve the security of the network.

(d) Require the use of encrypted passwords when available. This features should be implemented at the time the LAN is installed as it is most transparent to the users at that time.

(e) When employees are no longer part of the organization, or their duties change, their account access should be appropriately modified or terminated.

c. Unauthorized Access to LAN Resources

(1) List possible vulnerabilities, such as improper use of LAN manager, system operator (sysops) privileges, etc.

(2) Limit the number of individuals who have systems administrator privileges. The systems administrator should have a separate ID and password for exercising systems administrator privileges.

(3) Limit the number of individuals who have print queue management privileges. These personnel should have a separate ID and password for exercising queue management privileges. Ensure that personnel who possess this privilege are properly trained and monitored to ensure they do not use the print queue login only for its intended use.

d. **Disclosure of LAN Data**

(1) List possible vulnerabilities such as data stored in open area, data stored in unencrypted form, etc.

(2) Ensure that provisions for physical security of data in the work place are commensurate with the nature of the data to which users have access.

Physical controls used for an area should take into account those employees authorized to be in an area but who are not authorized access to sensitive information.

(3) Determine who has access to the work place during regular working hours to safeguard all information technology resources.

e. Unauthorized Modification of Data and Software

(1) List possible vulnerabilities, such as improper or unnecessary permissions granted to employees, viruses, etc.

(2) Restrict the access of users to the LAN by limiting their access to specific business hours only.

(3) Limit the number of active logins employees may use at any one time.

(4) Restrict employee access to the LAN by permitting them access from their workstation on his/her desk only.

(5) Employee workstation access to such network resources as the Internet needs to be addressed by use of firewalls or other such features. The Internet for all its usefulness is also an access point for virus infection.

f. **Backup of LAN Data**

(1) List critical data on the LAN and determine the frequency of backups, which should be performed at least weekly, or more often, depending on the nature of the data.

(2) Several generations of monthly backups should be retained and the restore process tested regularly to ensure that the LAN server disks can be restored to their original state.

g- **Disruption of LAN Functions**

(1) List possible vulnerabilities, such as inability to redirect LAN traffic, "single point of failure" LAN configuration, etc., to identify and prevent denial of service situations.

(2) During the design of the LAN architecture, plan system redundancy and system backup at critical junctures of the system. Good systems design improves continuity of operations prospects by not creating "a single point of failure" where the failure of one system component can bring down the entire LAN.

(3) List possible threats, vulnerabilities and resultant risks for assessment.

h. **Selection of Security Controls.** Security mechanisms, procedures, software, etc. should be installed on the LAN to control or reduce the risk resulting from threats posed by LAN weaknesses. These "Security Services" include the following:

(1) Identification and authentication. A mechanism that provides an assurance of the identity of an individual.

(2) Access Control. A mechanism to restrict use of system resources.

(3) Data Confidentiality. A process of keeping data secure.

(4) Data Integrity. A process to ensure that data is not destroyed or modified.

(5) LAN Message Confidentiality. A process of protecting the privacy of e-mail so that only the intended recipient(s) can read it.

(6) LAN Message Integrity. A process of protecting the contents of a message to ensure that it is not modified.

(7) Non-repudiation. A method which ensures senders and receivers of data cannot repudiate their processing of data.

(8) Logging and Monitoring. Audit trailing of specific system activities.

i. **Match Security Controls with Security Requirements**

(1) Determine the appropriate security services compared with risk of a threat and the cost for implementing a securi-ty mechanism that reduces a risk.

(2) Calculate costs for security mechanisms.

(3) Rank security measures.

j. **Implement and Test Security Mechanisms**

(1) Develop security controls implementation plan.

(2) Independently test mechanisms

(3) System test the mechanisms/controls.

(4) LAN security requirements should be reviewed.

(5) Risk should be reduced to lowest acceptable level.

4. **REFERENCES**

a. FIPS Pub 191, "Guideline for Local Area Network Security."

b. "Glossary of Computer Security Terms," National Computer Security Center, NCSC-TG-004, version-l.

REMOVAL 01' SENSITIVE DATA-
QUICK REFERENCE GUIDE

Prior to the release of a PC with sensitive data (as distinguished from the software which processes the data) stored on the hard disk, one of the following methods for removing or destroying that data must be applied. Select from the following acceptable options the method your office will use to accomplish this requirement:

1. If possible and permissible, remove the PC's hard disk (removable drive).

2. If removal of the hard disk drive is not feasible, the following procedures and techniques are recommended to remove or destroy sensitive data on the PC's hard disk(s):

a. Overwrite software. Overwrite software, which employs a computer program to write a pattern of characters (usually l's, O's, or a combination of both) onto the location of the storage media (hard disk) where the sensitive data is located, may be used to obliterate data on the PC. Overwriting using l's and O's should be performed at least twice on hard disks used to store sensitive data. After using overwrite software on a disk, the overwrite should be verified. This may be done by attempting to recover the data on the 'overwritten disk by using any one of several commercially available "data recovery utilities." Overwrite software is commercially available in most local computer retail stores and also appears on approved VA and GSA product lists.

b. Degaussing. Degaussing is a method to magnetically erase data from magnetic storage media, such as hard disks. Degaussing involves using an alternating current (AC) to generate a magnetic field to demagnetize the hard disk. Two types of degaussers are used: strong magnets and electric degaussers. Degausser products and equipment are tested by the DOD, approved by NSA, and then placed on NSA's Degausser Products List (DPL). If this method of data destruction is selected, contact a security specialist in the IR Security Office, in the Office of the DAS for IRM, for specific information on degausser options.

c. Destruction. Destruction of the media (hard disk) containing sensitive information may involve incineration, application of an acid solution, or processing at an approved metal destruction facility. When possible, sensitive information should be removed from the disk before it is destroyed. Most destruction methods or procedures involve potentially hazardous conditions and should be done only by qualified and approved personnel. Refer to NSA's NCSC-TG-025 Guide for specifics on this method and its applicability.

3. Document that sensitive data has been cleared from the PC being released.

57. Master Boot Record. The part of the boot area containing the partition table. Unless moved by a virus, it is stored in the Master Boot Record, on side 0, cylinder o, sector 1.

58. Memory. Solid state storage frequently used by the computer as a temporary working area.

59. Multipartite. A virus that has more than one method of infection. Usually a multipartite virus can infect boot sectors and program files

60. Network. Two or more systems connected by a communications medium; a network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

61. Non-repudiation. Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

62. Optical Media. A permanent storage media that uses laser technology to write to and read from a disk.

63. Overwrite. A procedure to destroy data recorded on storage media by recording null or random patterns.

64. Partition Table. A data table within the Master Boot Record. Created with FDISK, it keeps information on how the hard disk is divided or partitioned, including the size of each partition, its starting and ending point on the drive, etc. Floppy disks do not have a partition table.

65. Performance Training. Training that develops skills to design, execute, or evaluate Department computer security procedures and practices. of value, e.g., money, benefits, or medical care.

66. Program Virus. See "File Virus".

67. Release. To transfer control and custody of equipment.

68. Reuse. Refers to the subsequent use of FIP equipment after it is no longer needed for the purpose for which it was originally acquired.

69. Risk Analysis. An analysis of system assets and vulnerabilities to establish an expected lost from certain events based on estimated probabilities of occurrence.

70. Risk Assessment. A study of the vulnerabilities, threats, likelihood of loss or impact, and the theoretical effectiveness of security measures.

71. Risk Management. The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review.

72. Safeguards. The protective measures and controls that are prescribed to meet the security requirements as specified for an AIS. These safequards mav include but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls, management constraints; personnel security; and physical structures, areas, and devices.

DEFINITIONS

1. Access. The ability and the means to approach, communication with (input to or receive output from), or otherwise make use of any material or component in an ADP system or network. A user's ability to communicate with (input to or receive output from) a system or to have entry to a specified area.

2. AIS (ADP or Computer) Resources. Personnel and property associated with or accessible by an automated information system, office automation, and telecommunications medium, including information, data, locally-developed programs, equipment, facilities, supplies, services, and commercial off-the-shelf software.

3. AIS (ADP or Computer) Security. The combination of physical, administrative, and technical measures applied to protect AIS resources from loss, destruction, misuse, alteration, or unauthorized disclosure or access.

4. AIS (ADP or Computer) System. An assembly of computer hardware, software and firmware configured to collect, create, communicate, compute, disseminate, process store, and control data.

5. Authentication. The act of identifying or verifying the eligibility of a station, originator, or individual to access information. This measure is designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator

6. Automated Information System (AIS). An assembly of FIP resources configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

7. Availability (Data or System). The state that exists when computer resources are available (system is operational, data is accessible) to authorized users when they need it to accomplish daily operational and functional requirements.

8. Awareness Traininq. Training that creates the sensitivity to threats and vulnerabilities of computer systems and the recognition of the need to protect data, information, and the means of processing them.

9. Boot Area. A general term that includes both the Master Boot Record and the System Boot Sector. A floppy disk always has a System Boot Sector, and a hard disk has both a Master Boot Record and a System Boot Sector. See "Boot Record."

10. Boot Record. A short bootstrap program used to load the operating system. The boot record can be anywhere on the hard disk, depending on how the hard disk is partitioned with Fdisk, the DOS command which starts the Fdisk program that configures the hard disk for use. Usually, it is the first sector of the partition side 1, cylinder 0, sector 1, The boot record is always located in the system boot sector, unless moved by a boot virus. On a floppy disk, the boot record is always on side 0, cylinder 0, sector 1. See "Boot Area."

11. Boot Virus. Virus which infects and spreads by infecting the hard drive's Master Boot Record and/or System Boot Sector.

12. Business Impact Analysis. The first step in the contingency planning process. The quality of analysis will directly impact the cost and adequacy of recovery capability. The outcome ~1~11 cost justify planning and dictate recovery strategies.

13. Business Resumption Planning. Planning that enables an organization to return to normal operations.

14. Check Sums. One thing viruses have in common is that they all modify the disk. By infecting a file or boot sector, the disk has been modified. A check summing program, as used to detect computer viruses, would keep a mathematical score for each program file and boot sector, and if altered in any way then a virus would be suspected. Programs and boot sectors are not generally modified. This is considered to be the most useful of all anti-virus methods, though it can be time consuming.

15. Companion Virus. A virus that exists as a whole program file. It is executed instead of the intended legitimate program the computer user intended to execute by having the same program name but with a COM extension (COMs execute before EXEs). The virus then executes the originally intended program. Viruses that modify the directory's program starting cluster information so that a virus can be executed instead could be considered a form of companion virus.

16. Compromise. A violation of the security of a system such that unauthorized disclosure of sensitive information may have occurred.

17. Computer Abuse. The intentional and improper misuse, alteration, disruption of destruction of data processing resources.

18. Computer Fraud. Computer-related crimes involving deliberate misrepresentation, alteration or disclosure of data in order to obtain something

19. Computer Matching. The automated comparison of two or more sets of data files to search for individuals or entities included in both or all sets.

20. Computer Security Plan. A plan for computer systems that contain sensitive information. It is composed of a basic description of the purpose, environment, and sensitivity of the system, along with the security measures intended to protect the system and its data.

21. Confidentiality. The computer security characteristic that ensures individuals are given access to computer resources based on security clearance and need-to-know. This characteristic protects against compromise and inadvertent disclosure.

22. Contingency Planning. A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operation in an emergency situation.

23. Contingency Planning Team. The personnel who develop the contingency plan.

24. Contingency Response Team. The personnel who initially respond to the disaster.

25. Copyright Infringement. A violation of or trespass on the legal right of another to reproduce, publish, and sell the matter and form of literary, musical, or artistic work. This definition applies to computer software.

26. Critical Functions. The functions performed by an organization in order to fulfill the mission of an organizational element.

27. Customer- A person or organization who receives products that an automated system produces, but who does not have access to the system.

28. Data Confidentiality. A process of keeping data secure.

29. Data Integrity. A process to ensure that data is not destroyed or modified.

30. Data Remanence. The residual physical representation of data that remains on storage media after erasure.

31. Degausser. An electrical device that can generate a strong magnetic field that is used to bulk clear (also known as a "bulk erasure") or erase magnetic storage media.

32. Disposal. Release of ADP equipment to be excessed, transferred, discontinued from rental/lease, exchanged, or sold.

33. Encrypted Virus. A virus that rotates bits or uses some other form of encryption so that it is no longer readable by any virus signature scanning software, making it difficult to detect or identify.

34. Erasure. A process by which data recorded on storage media is removed.

35. Executable Files. Program files that can be "run" to instruct the system what to do. The file types are designated by the type of extension on the file. Examples include: APP, COM, BIN, EXE, DLL, OVR, OVL, and SYS files.

36. Facility. A site or location where information processing is performed, locally or remote, including VA Automation Centers, Information Systems Centers, clinical laboratories, regional offices, and medical centers; or where data or information from such sites are stored for security, vital records, or emergency preparedness purposes.

37. File Allocation Table (FAT). A table of the starting location of programs and files on every disk. The FAT is often a target of viruses that erases the FAT and renders the data on the disk inaccessible.

38. File Virus. A virus which infects and spreads through program files (executable files). They are operating system dependent, and mostly machine independent. This means that they thrive on PC-DOS and MS-DOS, regardless of which computer the operating system is running on.

39. FIP Equipment. Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display. switching, interchange, transmission, or reception of data or information.

40. General Support Systems. Systems which consist of hardware and software that provide general ADP or network support for a variety of users and applications.

41. Generic Differential Detection. See "Heuristics."

42. Heuristics. A method of looking for computer viruses by their characteristics rather than signatures or check sums. The benefit of this type of anti-virus technique is that it is able to detect viruses that it has not been programmed specifically to de:ect (such as in the case of a signature scanner). Also known as Generic Differential Detection or Holistic scanning.

43. Holistic scanning. See "Heuristics."

44. Identification. The process that enables recognition of a user described to an ADP system. This is generally by the use of unique machine-readable names recognition of users or resources as identical to those previously described to an ADP system.

45. Incident. Any act or circumstance that involves sensitive information that deviates from requirements of governing security policy and procedures. For example, comprise or unauthorized disclosure of sensitive information.

46. Incident Response and Security Team. Personal organized to make the initial response to an incident, identify the problem, and recommend interim and permanent solutions.

41. Information Resources Security Officer (IRSO). The designated individual in VA who is responsible for automated information system (AIS) security for the Department.

48. Information Security Officer (ISO). The individual in a VA Administration, staff office, or facility who is designated responsible for establishing and implementing AIS security procedures. These procedures are based upon Department, Administration, and staff office AIS security procedures and guidelines.

49. Initial Security Training. Security training that new employees are required to attend within 60 days of their appointment. Employees receive an introduction to the basic concepts of computer security practices and the importance of the need to protect the information from vulnerabilities to known threats.

50. Integrity. A computer security characteristic that ensures computer resources operate correctly and that the data in the data bases are correct. This characteristic protects against deliberate or inadvertent, unauthorized manipulations. This characteristic is applicable to hardware, software, firmware, and the data bases used by the system.

51. LAN Message Confidentiality. A process of protecting the privacy of e-mail so that only the intended recipient(s) can read it.

52. LAN Message Integrity. A process of protecting the contents of a message to ensure that it is not modified.

53. Local Area Network (LAN). A short-haul data communications system that connects ADP devices in a building or group of buildings within a few square kilometers, including (but not limited to) workstations, front end processors, controllers, switches, and gateways.

54. Logic bomb. This is the portion of the virus that does the damage, such as wiping out hard disks, destroying File Allocation Tables (FAT), deleting files, modifying data, etc. It could also be something less harmful, such as a taunting message, falling characters, etc. See "Trigger."

55. Logging and Monitoring. Audit trailing of specific system activities.

56. Macro Virus. A computer virus that is written in a macro programming language such as those included in many spreadsheet and word-processing programs. Originally intended to allow the software user a way of automating repetitive tasks the increased sophistication of these macro languages also allows the development of malicious macro programs or even programs that can be technically called computer viruses.

73. Scanner. (Virus scanner) Anti-virus software designed to search the contents of program files and disks usually looking for sequences of bytes thought to be unique to certain viruses. Anti-virus software that relies solely on this method for detection should be updated monthly (or as provided by the anti-virus software manufacturer), as the currency of software and its included signature database is critical.

14. Security Cost/Benefit Analysis. The valuation of the degree of risk reduction that is expected to be achieved by implementing the selected risk-reducing measures. The gross benefit, less the annualized cost to achieve a reduced level of risk, yields the net benefit.

75. Security Safeguards. The protective measures and controls that are prescribed to meet the security requirements for an AIS. These safeguards may include, but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices.

76. Sensitive Data. Data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability to accomplish a mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act.

77. Sensitive Information. Any information, the loss, misuse, modification of, unauthorized access to, or disclosure to the public, that could affect the national interest or the conduct of VA programs. Information loss, misuse, modification of, unauthorized access to, or disclosure to the public, that could affect the privacy to which individuals are entitled under the Privacy Act, Section 552a of Title 5, United States Code, or which is protected under any other confidentiality statute, such as 38 U.S.C. Sections 5701, 5705 and 7332. This designation covers information that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

78. Signature. (Virus signature) A sequence of bytes thought to be unique to a particular virus. The "signature" can be used by scanning software to search suspect files and disks for a specific sequence. If the sequence is found, then that file or disk is thought to be infected by that particular virus. Also known as a virus fingerprint.

79. Software Copyright. The right of the copyright owner to prohibit copying and/or issue permission for a customer to employ a particular computer program.

80. Solid-state "Hard Disk". Solid state storage device using "flash" memory chips (non-volatile) used by the computer for permanent (long term) storage, duplicating the functionality of a fixed or hard disk.

81. Stealth. Any technique used by a virus to conceal itself while in memory.

82. Storage Media. Automatic data processing equ ipment with permanent magnetic/optical/solid-state propertiea which are used by the computer for permanent (long term) storage.

83. Threat. Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.

84. Trigger. The programming logic built into a computer virus that causes it to attack. This could be a certain date, like Friday the 13th, when the hard disk data is destroyed, or some other factor or combination of factors. See "Logic Bomb."

85. (End) Users. Any employee or other customer who has access to a Department computer system that processes sensitive or non-sensitive information. This is the largest and most heterogeneous group of employees. It consists of everyone from the data entry clerk who has a personal computer with sensitive information to the executive.

86. Virus. A self-propagating Trojan Horse (a program that surreptitiously exploits the security/integrity of a program), composed of a mission component, a trigger component, and a self-propagating component.

87. Vulnerability. A weakness in automated system security procedures, administrative controls, internal controls, etc., that could be used as a threat to gain unauthorized access to information or disrupt critical processing.